Are You Ready for the New Identify Theft Regulations?

The federal financial services regulatory agencies have developed new rules and guidelines to require financial sector organizations, including the mortgage industry, to better protect consumers from identity theft. The new rules, which are outlined in the Fair and Accurate Credit Transaction Act (FACT Act), were effective on January 1, 2008, with mandatory compliance by November 1, 2008.

Basically, each financial services company and creditor that holds any consumer account, where there is risk of identity theft, must develop and implement an identity theft prevention program for combating identity theft in connection with new and existing consumer accounts. It is important to note that there is not an easy off-the-shelf solution to be implemented. The regulators will be looking closely at how each organization implemented its identify theft program.

The first step in creating an identity theft program is to conduct a risk assessment. The purpose of the risk assessment is to determine the extent of the need of the identity theft program and to specifically identify the accounts the program must address. The next step in the program development is to document the relevant patterns, practices, and specific forms of activity that are the "red flags" that signal possible occurrences of identity theft. Red flags are risk events, which with appropriate controls, will be prevented from occurring and/ or detected if occurred. The identity theft regulations provide 26 red flags examples to be considered for the organization's red flag library. These 26 red flags are considered a starting point. The regulations require an in-depth review of the organization to develop a red flag library that is specific to the organization.

Following the red flag identification step, the next step is to develop procedures to prevent and detect red flags, as well as providing for an effective response to the red flags. Preventative controls are the most ideal controls, but typically are more expensive to implement than detective controls. As with any control implementation, the benefits of the control should exceed the cost of the control. When determining the cost/benefit of controls, one should not forget about intangible benefits, such as the avoidance of the reputational harm due to a breakdown in identity theft controls.

Mortgage Identity Theft

Identity theft continues to be a significant problem in the mortgage industry. The April 2008 report, *Mortgage Loan Fraud,* published by the Financial Crimes Enforcement Network (FinCEN) reported that suspected identity theft in conjunction with mortgage fraud increased 97% from their previous study in 2006.

Mortgage identity theft involves an attempt to obtain credit using another person's identity. In other words, it involves the misuse of information with the intent to deceive or mislead the lender into extending credit that the lender would not have likely offered if the true identity had been known. The fraud perpetrators abscond with the proceeds of the loan with little or no intention to purchase or occupy the house. Victims of mortgage fraud identity theft have had their properties encumbered with loans or property titles fraudulently transferred, effectively having their homes stolen.

In their April 2008 report, FinCEN provides some real world examples of mortgage identity theft:

- Individuals stole the identities of a property owner to allow them to sell the property to another individual who assumed the identity of another true person. In this scheme, the existing mortgage on the property was paid off with a new mortgage. The perpetrators received the difference between the sales price and the loan payoff. This fraud scheme is

more profitable when perpetrated against homeowners with a large amount of equity in their home. The legitimate homeowners discover the fraud when they are informed that their mortgage has been paid in full.

- Homeowners' identities are stolen to apply for home equity lines of credit or cash-out financing. In this scheme, the borrower applies for multiple loans from multiple lenders on the same property in a short period of time. This allows the identity thief to take advantage of lag time in recording the mortgages. Consequently, the lenders are unable to identify the existence of the other loans. By the time the lender is aware of the other mortgages, the loan payment has already been provided. First payment defaults are the first sign of trouble.

Red Flags

Before an identity theft program can be successfully prepared for a mortgage operation, management must confidently recognize any red flags that are relevant to their organization. There is not a standard list of red flags that will apply to every organization. The organization's guidelines, products, and procedures will make some red flags more prevalent and others non-existent. Some common red flags surrounding identity theft used to facilitate mortgage fraud are:

- Consumer credit report contains one of the following – fraud alert, active duty alert, notice of credit freeze, address discrepancy, significant number of recent inquiries, an unusual number of recently opened accounts, or accounts that were closed for cause or abuse.
- Identification documents and/or application (1003) provided appears to be altered or forged.
- Signatures on documents are not consistent throughout the loan file.
- The social security number provided was never issued or does not match the credit report.
- The phone number provided is not valid or is associated with a pager or answering service.
- The proposed borrower is not able to provide documents (asset or employment documents) that would verify information provided on the application. Borrower requests mail be sent to "work" address.
- Return mail received on RESPA disclosures or first statement sent.

Controls

All mortgage loan operations will handle customers' personal identification at some point in the origination process. The handling of this information can make a difference to the operation's bottom line, as well as the lives of their borrowers. Solid internal controls designed around customized red flags will help any organization avoid the substantial financial losses that always follow mortgage identity fraud. These controls should consist of security, prevention, detection, and response measures. Organizations should consider using automated IT tools, as well as checklist, suspicious party list, and unbiased, third party reviews to assist in the execution of their internal controls. Internal control measures should be present during the origination, processing, underwriting, closing, and funding functions with each specific identifying data piece (address, social, name, etc.) verified a minimum of three times prior to the funding of the mortgage loan.

Best-in-class lending organizations rely heavily on submitting brokers to perform proper independent due diligence on all loan applicants, including a re-verification of loan documents. It can be as simple as making sure that the borrower's signature matches on all documents, all parties in the transaction present acceptable photo identification, and all documents are signed in front of a licensed notary public.

Identity theft mortgage fraud can be detected in various phases of the loan process: pre-funding, post closing audit, loan default, and through reports by victims, law enforcement and even the borrowers themselves. Obviously, prevention of the fraud is ideal through an effective internal control system. But if the fraud occurs, then detecting the fraud at the earliest possible point, ideally before funding, is best.

Automated IT Tools

There are many automated IT tools that mortgage companies can use to detect potential identity theft used to facilitate mortgage fraud. The increase in mortgage fraud over the last several years has led many mortgage software vendors to enhance their product offerings. This is especially true in the area of identity fraud. These tools are offered by several established vendors and are often web-based, which provides convenient integration into the origination process. Some of the more robust tools provide the following:

- Social Security number validation including checks for state issued, age and death reconciliation, and multi-use;
- Name variances including all aliases utilized;
- Office of Foreign Assets Control (OFAC) list checks;
- Drivers license number validation;
- Assessment of the borrower information history to detect unusual patterns that are highly correlated with mortgage fraud

Conclusion

Creating an effective and customized identify theft program, which will pass the scrutiny of the government regulators, requires a lot time and effort by the organization's compliance team and management. No doubt, in today's regulatory environment, with more and more regulations being written and dealing with multiple deadlines and exams, this can be overwhelming. The new identify theft regulations can bring the feeling of just one more regulation that has to be addressed. But, with the proper tone and commitment from organizations' board of directors and executive management, an effective identify theft program can be put in place that protects your organization's customers from the horrible hardship of having their identity stolen. And this makes perfect business sense.